INCORPORATING DIGITAL WATERMARKS IN COLOUR DIGITAL IMAGES

M.A. Chapman[1], A. Fidera[2]

Geomatics Engineering, Department of Civil Engineering,
Ryerson University, Toronto, Canada
[1] mchapman@ryerson.ca,
[2] afidera@ryerson.ca

Commission II, IC WG II/4

ABSTRACT:

A digital image can be watermarked for security purposes by taking a coded digital record and embedding it to the digital image in such a manner that it cannot be easily detected or removed. The record that becomes the watermark is often a recognizable logo. Using variable parameters entered by the user, the logo is mixed using a watermark algorithm until it appears as no more than random black spots. These spots can be inserted into the digital image as background noise, and just as easily removed if the input parameters are known. If the watermark is removed and the logo is not intact, then it suggests that the digital image has been altered from its original state.

Digital images have been routinely used in such areas as remote sensing, backdrops to CAD drawings, and medical imaging. The digital image is often of considerable value or contains information that is crucial for a particular application. Therefore, ensuring its authenticity and ownership is of considerable importance.

1. INTRODUCTION

This paper presents the results of research performed with respect to digital watermarking and imbedding digital codes in colour digital imagery. The primary problem to be addressed is associated with the encryption of watermark information in such a manner that it remains undetectable, has minimal effect on the original image and that it is extractable. These various criteria must be adequately addressed in order to ensure that the watermarking process has a high level of integrity and is robust in terms of its resistance to tampering.

This paper presents as a primary focus the results of the research done on digital watermarking. Application of the method to georeferenced images is discussed. Both watermarking and georeferencing are additions that, if implemented in digital survey plans, serve to enhance the product being offered to users.

2. BACKGROUND FOR DIGITAL WATERMARKS

Government agencies, private enterprises and individuals have been routinely using digital imagery in their day-to-day operations. In many ways, images that are stored digitally are the same as those that were previously stored on paper, but the storage medium is now an electronic file rather than photographic paper or Mylar, for example. Digital images are stored as computer files with a specific graphical format. A difficulty that exists in using computer files as official documents, as for example legal records, is that a computer file's content can be easily altered. Consequently, there must be a security procedure that offers protection for copyright and that prevents unauthorized alteration of digital files.

This topic of image security in the surveying community was discussed by Broadus (1999), who describes the use of digital signatures for protecting the integrity of digital plans. Digital signatures are a more general definition of digital watermarking, with the same objective, of securing the image against manipulation. Mr. Broadus reviews the trends in different US states towards use of digital signatures in all electronic communications. From conversations with Land Surveyors, Mr. Broadus states that very few have adopted the habit of adding a digital signature to their electronic correspondence, although there is no real obstacle preventing them from doing so. The most likely result will be that the procedure will be eventually mandated by legislation.

Watermarking computer images is a new area of research but it has roots in older disciplines. Hiding messages inside other messages, commonly used during times of war, is known as steganography, which is derived from the Greek word meaning 'covered writing'. Marking an image such that the human eye cannot notice the additional marks requires comprehension about visual perceptibility limits. Knowledge of digital image processing techniques and information transmission methods are also required. In order to construct a mathematical algorithm that is secure, meaning that it cannot be easily deciphered, the watermark inventor must possess understanding of advanced mathematics and statistical probabilities.

3. DIGITAL IMAGES AND WATERMARKS

Different watermarking methods perform better when certain assumptions are made about the format of the document to be watermarked. Digital representations of paintings, for example, are usually in colour format, with eight or more bytes representing each pixel. Therefore, there is high variability between pixels. Watermarking algorithms for colour images usually operate by applying subtle variances to pixel colours that cannot be discerned by the human eye. These watermarking techniques may be applied to both grey-scale as well as colour images. (note: A graphics file can be saved as a black and white image, a greyscale image, or as a colour image, thus requiring 1 bit, 1 byte, or multiple bytes, respectively to store each image pixel.) For example, many survey plans are recorded in black and white, which requires only one bit per pixel. Plans are often uniformly white through much of the background of the image, making survey plans extremely simple images from a graphical viewpoint. It is much more difficult to hide a watermark within a survey plan because, in a sense, there is nothing to hide behind. Most existing watermarking schemes are, therefore, not applicable to survey plans encryption.

A general watermarking method that is applicable to a variety of digital image formats must be sufficiently adaptive and robust. For example, many digital images are recorded as TIFF (Tagged Image File Format) files. It is this TIFF file then that is the document to be watermarked, as this is the official document. The version of the image prepared by the user, regardless which software package (or format) is used, may be considered the official registered version. Thus, it may be a TIFF file converted from these original versions that becomes the official document. TIFF images can be used on all major platforms (Windows, Macintosh, UNIX, etc.). It allows storage of multiple bitmap images in one file and supports multiple compression algorithms. With the latest release supporting 12 different data types that may be best represented as bits, bytes, integers, unsigned integers or even strings of indeterminate length. Compressed image formats pose different problems and will not be discussed further here. TIFF is one of the most versatile graphics file formats currently available.

However, many users constrain images to specific formats as dictated by their intended applications or regulations. The images may also be stored each time in a different format. The versatility of the TIFF graphics format may be of importance to the user. The watermarking technique now to be discussed below was chosen because it was possible to adjust the technique so that it was applicable to a specific format required by the user.

4. THE DIGITAL WATERMARK

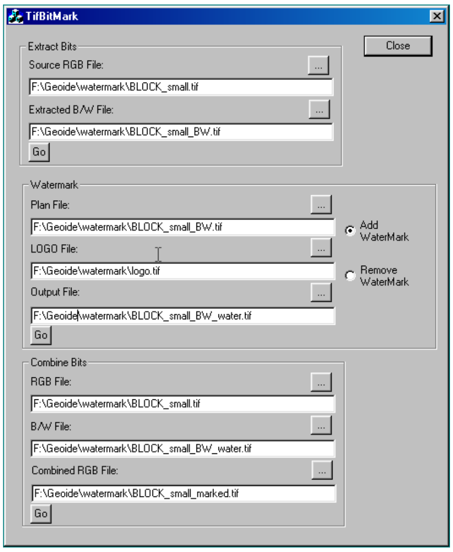
This section discussed the watermark that was developed to work colour or grey-scale digital. In 1998, Voyatzis and Pitas presented an algorithm for watermarking an image and the watermarking technique developed here was derived from this algorithm.

The Mixing System method presented by Voyatzis and Pitas while applicable to either greyscale or colour images will be initially discussed in the context of grey-scale images. Their method is more specific than the method currently being presented. In discussion of the method used to watermark digital images, the spirit of the Mixing System method is visible with appropriate deviations for the purposes of versatility and robustness.

To demonstrate the successful application of the mixing method, a program was written that performs the mixing procedure. The discussion here refers to outputted images from that program. An illustration of the user interface menu is given in Figure 1.

In the example to be presented, a binary logo (Figure2) will be used to generate the watermark to be inserted into a digital document or image.

The procedure of watermarking a digital image requires that the identifiable image be transformed and resized into a watermark that can be hidden appropriately within the original image.



Source RGB File: F:\Geoide\watermark\BLOCK_small.tif

Extracted B/W File: F:\Geoide\watermark\BLOCK_small_BW.tif

Plan File: F:\Geoide\watermark\BLOCK_small_BW.tif

LOGO File: F:\Geoide\watermark\logo.tif

Output File: F:\Geoide\watermark\BLOCK_small_BW_water.tif

● Add WaterMark

○ Remove WaterMark

RGB File: F:\Geoide\watermark\BLOCK_small.tif

B/W File: F:\Geoide\watermark\BLOCK_small_BW_water.tif

Combined RGB File: F:\Geoide\watermark\BLOCK_small_marked.tif

Figure 1. User Interface Menu

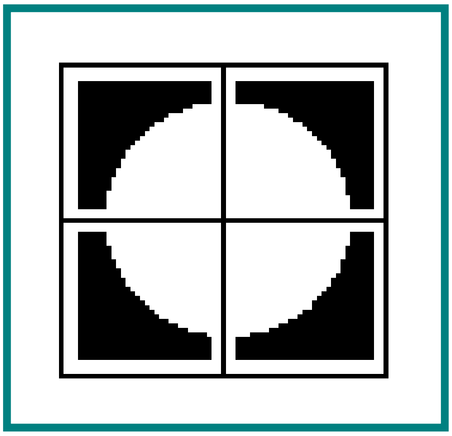


Figure 2. Sample Logo

As a first step, a logo image is taken, and by using a mixing equation, all pixels in that logo are uniquely relocated. Every pixel is located in an image by (x, y) or (column, row) coordinate values. To relocate theses pixels and, thereby, mix the image, each pixel is repositioned (thus preserving the original grey values) by multiplying the original x and y by a 2x2 matrix which produces new x and y values, as seen in the following equation:

$$\begin{pmatrix} X_{NEW} \\ Y_{NEW} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ K & K+1 \end{pmatrix} \begin{pmatrix} X_{ORIGINAL} \\ Y_{ORIGINAL} \end{pmatrix}$$

The mathematical foundation for the Mixing System method is the 2x2 matrix that conforms to the condition that the matrix determinant is equal to one [i.e., $(K+1)-k=1$]. The parameter K in the equation is the mixing parameter. K can be any positive integer value chosen and entered by the user.

Applying the above equation without further constraints would result in a new mixed image of larger dimensions than the original. In the x-direction, the dimensions would increase by (Xmax + Ymax). In the y-direction, the dimensions would increase by (K*Xmax + (K+1)*Ymax). To regulate the image size, the equation above must be multiplied by a modulus of the maximum desired dimension of the image. The outputted result will be a matrix of size "Dimension", yielding the following expression:

$$\begin{pmatrix} X_{NEW} \\ Y_{NEW} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ K & K+1 \end{pmatrix} \begin{pmatrix} X_{ORIGINAL} \\ Y_{ORIGINAL} \end{pmatrix} \bmod \mathit{Dimension}$$

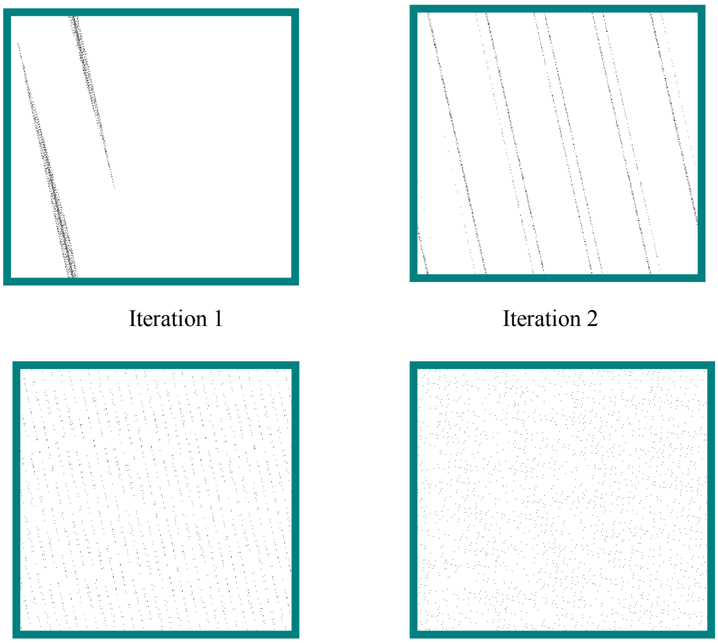
To mix the watermark extensively, the above equation can be reapplied to the resultant mixed logo, allowing an iteration procedure to develop. In the program written, the size of each mix result was maintained as a matrix of size M, the maximum dimension of the logo. Every successive iteration serves to more extensively mix the original logo pattern, and each iteration produces a new matrix. The number of iterations 'r' is an integer parameter chosen by the user.

Figure 3 shows the results of the first few mixes (iterations). When the iteration procedure is complete, a final mix is performed in which the dimension parameter is changed from M, the maximum dimension of the logo, to N, the minimum dimension of the recipient image that is to be watermarked. To ensure maximum encryption performance, N should be larger (>2x) than M.

The final overlay involves two steps (see Figure 4). During Step # 1, the mixed logo is resized to the larger NxN dimensions. The watermark is now in the form required for application. A final parameter 's', the shift parameter, is chosen to displace the watermark coordinates relative to the image. A second shift parameter applied in an orthogonal direction could also be used although this option was not used here. The mixed logo is overlaid onto the recipient image during Step # 2, shifted by the amount 's', and the original image is then watermarked. In summary, the mixing of the logo is achieved by randomly choosing the set of mixing parameters discussed above: K - the mixing parameter, r – the iteration parameter, and s – the shift parameter. The dimension parameters, M from the logo size, and N from the original image size, should also be noted in case the watermark must later be removed.

5. COLOUR IMAGES

The previous discussion focussed on the concept of encryption in the context of grey scale images. The extension of this methodology to colour images is relatively straightforward although several variations of its implementation are available. The approach favoured in this research involved the selection of one of the three channels in, for example, an RGB-based colour image. Histograms of an illustrative image are given in Figure 5.



Iteration 1

Iteration 2

Iteration 3

Iteration 4

Figure 3. Iteration Results

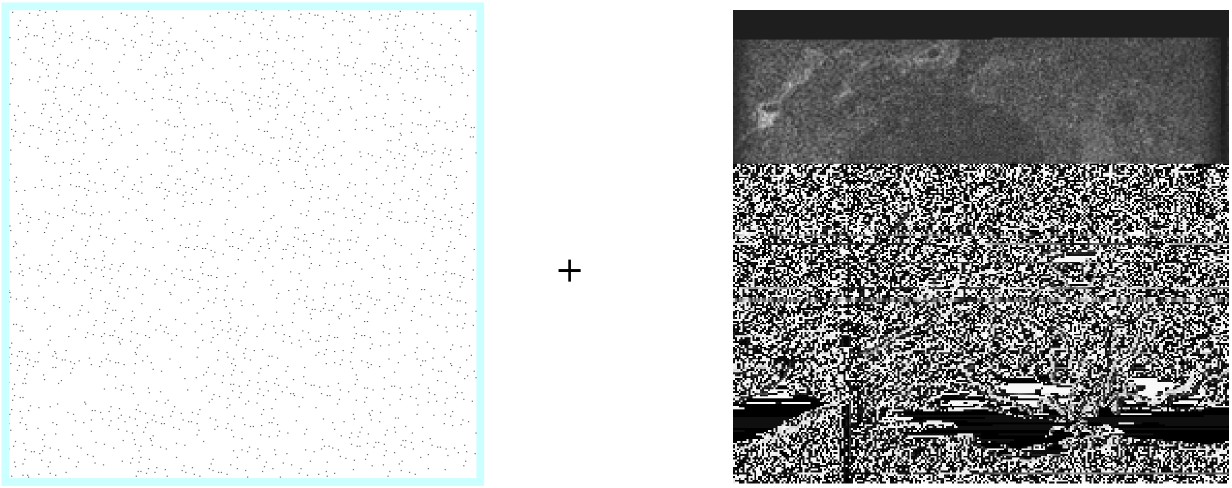
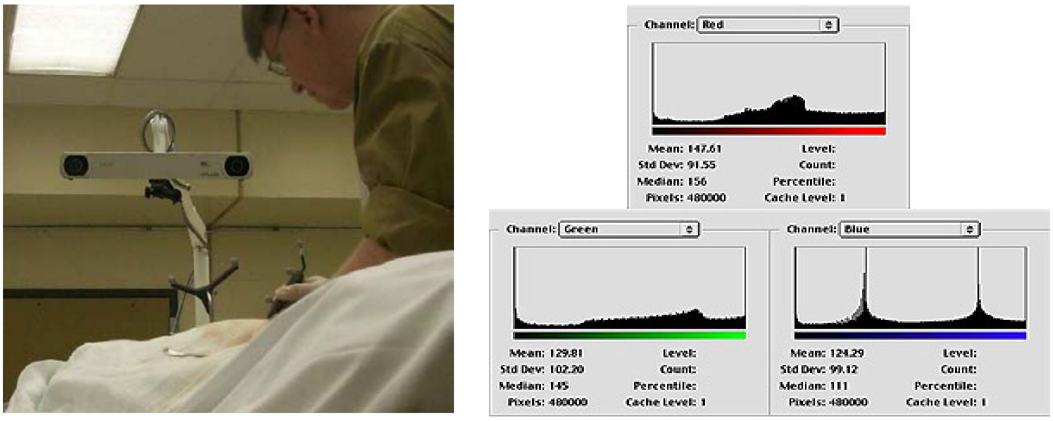


Figure 4. Mixed Logo and Recipient Image



```
Channel: Red
Mean: 147.61        Level:
Std Dev: 91.55      Count:
Median: 156         Percentile:
Pixels: 480000      Cache Level: 1

Channel: Green
Mean: 129.81        Level:
Std Dev: 102.20     Count:
Median: 145         Percentile:
Pixels: 480000      Cache Level: 1

Channel: Blue
Mean: 124.29        Level:
Std Dev: 99.12      Count:
Median: 111         Percentile:
Pixels: 480000      Cache Level: 1
```

Figure 5. Colour RGB Image and Channel Histograms

The lowermost bits of each of the three channels represent high frequency information that is often associated with noise. As such, the encrypted logo (which is binary in nature) can be used to replace the lowest bit of one of the three channels as defined by the user. For the purposes of this discussion, the green channel was selected as the recipient of the encrypted logo. By choosing one of the three available channels, the user has one additional means of "hiding" the watermark. Encryption could occur on all three channels if the user so desired.

6. DEWATERMARKING

If the parameters above are known, the logo can be removed as easily as it was attached. In the program, the user chooses the Dewatermark routine and the five parameters, K, r, s, M and N (as well as the channel in the case of colour images) are requested as input. With the parameter available, the program then replicates the steps of watermarking the image, following the entire mixing procedure. The program copies the value found in the encrypted image instead of inserting a value, and inserts this vale into its original position in the logo. In this manner, the entire logo is rebuilt or recovered. If the original image has not been altered the logo will be intact in the rebuilt file. Assessment of the extracted logo then determines if the image has been altered.

7. IMBEDDING GEOREFERENCED IMAGES

In some applications, it is proposed to use large-scale digitized aerial images as a background for survey plans (Williston et al, 2000). This idea is based on the premise that many of the end-users would find survey plans more useful if they had recognizable features available when viewing the line-work on the plans. Georeferencing of digital images with survey plans is a feasible concept irrespective of whether the plans are recorded in a digital or Mylar format. With current processing power and storage, it is now a relatively simple addition to survey plans to ensure that the background images are georeferenced. The process of georeferencing has been enhanced with the use of orthrectification, which is a process that employs the topography expressed in a digital form. The image displacement caused by the topography can then be removed during processing. However, certain residual discrepancies may persist due to the presence of artificial features.

The point to be emphasized is that an imbedded georeferenced image would represent an enhanced product relative to that currently being offered as survey plans. Survey plans should have imbedded images if they are to remain current with other mapping now being produced by other spatial data producers. A complete discussion of georeferencing is found, for example, in the paper by Cosandier and Chapman, 1995.

8. CONCLUSION

Watermarking of digital images is simply a next step in the process of converting from paper to digital format that has been ongoing in all areas since the computer revolution began. Broadus noted that, "digital signature technology does a better job of protecting the integrity of a document than does a paper signature". (Broadus, 1999, p.68). Digital watermarking is more robust than traditional watermarking and the stamp of a surveyor or engineer.

The method demonstrated here is applicable to various types of digital images currently used. This research demonstrated a robust and adaptable watermarking algorithm that can find application in many areas. Such an approach lends itself to use by many users with limited knowledge of the underlying watermarking principles or the recording techniques associated with many proprietary formats such as TIFF.

ACKNOWLEDGEMENTS

The programming contributions of Todd Williston, Peter Tate and Haibin Dong are gratefully acknowledged.

REFERENCES

Broadus, Jerry R,1999. The Surveyor and the Law: Update on Digital Signatures. *POB*, Sept., pp. 68-72.

Cosandier, D. and M.A. Chapman ,1995. Precise Multispectral Airborne Pushbroom Image Georectification and DEM Generation. I*SPRS Workshop, Integrated Sensor Orientation: Theory, Algorithms & Systems, Barcelona*, Spain, Sept. 4-8.

Voyatzis, G., and L. Pitas ,1998. Digital Image Watermarking Using Mixing Systems. *Computers & Graphics*, Vol. 22, No. 4, Elsevier Science Ltd. pp. 405-416.

Williston, G.T., M.A. Chapman and B.A. Ballantyne,2000. Enhancing Survey Plans in Alberta: Digital Watermarking and Georeferenced Images, *The Ontario Land Surveyor,* Vol. 43, No.1, Spring, pp. 8-10.